Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1801 01/01/16

~ N. Korea's Red Star OS ~ People Are Talking! ~ Firebee News Update!
~ EA, Steam Servers Down ~ The Internet of Things! ~ Chinese Email Hack!
~ Raspberry Pi Bribe Try ~ Eureka Lite Is Released ~ AVG Breaks Chrome!

~ Bogus Facebook Posts! ~ Bug Sets Prisoners Free ~ Ian Murdock Dead!

-* New Firebee Boards Ordered! *-
-* Where To Sell Unwanted Video Games! *-
-* New Atari Jaguar Controller in Development *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Happy New Year!!

As I was changing the dates of A-ONE’s masthead, I was amazed when I realized that we’ve been around for 17 years, starting our 18th! I still remember the few phone conversations that Joe Mirando and I had thinking about breaking away from STReport and starting our own online magazine. A lot of things have changed over the years! Surely, we knew that Atari-related news wasn’t going to be abundant. We weren’t even sure that we’d be around for very long, but we managed to do things a little bit differently, and hung around for awhile.

While Atari-related "news" was almost non-existent, we decided that our readers (or potential readers) would still be interested in seeing articles that were newsworthy and entertaining - stuff that we might not see or hear in the mainstream news outlets. So, we focused more on that while trying to include anything that pertained to Atari. And here we are, the beginning of 2016, and people are still out there using Atari hardware, working on some software and hardware - and, in general, still enjoy using the Atari platform.

I still have much of my old Atari computers and software; I just don’t use it any longer. One of these days - if I ever have the extra space - I’d like to set up one of those machines and play around with stuff that I enjoyed using for many years, back in the day! I know, famous last words! But, we’ll see!

Until next time...

=~=~=~=

FireBee News Update

By Fred Horvat

It was a busy week this week with the FireBee. I realized

something this week that I had missed the passed couple of months while owning the FireBee that makes a huge difference in using and getting support. I never clearly stated on http://www.atari-forum.com/ when asking for help was how I wanted to use my FireBee! People were offering great suggestions for what they were familiar with in their own personal use of the FireBee. This normally is not always how I want to use my FireBee. This week it made a difference and now has created some extra work for me on my FireBee. Last week I was discussing my DIP Switch Settings and how I put Switch #5 to the Off position to boot into EMTOS and how it has introduced a new problem of the system not always booting properly. It took me some time to think through it as others on the forum thought is was the brand of CF Card I was using.

To get the FireBee to boot back into FireTOS and stop the endless rebooting I did the following:

1: Checked all the DIP Switch settings and made sure all were set back to factory settings and made sure that #5+#6 were on. System still did not start up properly.
2: Shut down and pulled the CF Card out. Booted and still not working properly.
3: Shut down and removed USB keyboard and mouse and used TT keyboard and mouse. Booted and still not working properly. TT Keyboard did not work at the TOS Selection Menu. Strange thing I noticed was that with no CF, USB, or SD card the system was still booting into something and would say "Starting Auto Folder" and then crash. Since the TT Keyboard was not recognized I could not select what TOS to run.
4: Shut down and put a blank SD card in and started up. TT keyboard did not work so I attached a USB keyboard and mouse and selected EMUTOS. System started up into EMUTOS Desktop and was stable. I shut down and removed the TT keyboard and mouse. Booted up into TOS404 full and got the Desktop and it seemed stable. Shut down and put my normal SD and CF cards back in and booted up normally like I would and selected #1 at the TOS menu for TOS404 for MiNT and the system seems to be working now.

It appears to not be releated to the brand of CF Card I am using after doing these steps plus the CFs I have been using have been working great up until I changed DIP Switch #5 to Off. I can get the FireBee running again but the bug still exists at times. Instead of doing all the steps above I just boot into EMUTOS once and then reboot into FireTOS for MiNT and the system runs fine.

My next step is to reflash the firmware and put the original BaS that came with the FireBee and not the latest version. I ll see if that corrects the problem. Another user on the forum Orion seems to have the same bug with his FireBee that I was unaware of until it happened to me and someone pointed this out. Now that it is a known reproducible bug hopefully in a future Firmware update this can be addressed. Also if Orion or myself find a fix we can let the other and others know of our fix.

So like I stated at the beginning of this article I not been specifically clear in what I wanted to accomplish with my FireBee which this week led me down the wrong path. I looked at many different sources and listened to many user’s opinions. In the end it was entirely my fault in putting Switch #5 Off and booting

into EMUTOS. Somehow this introduced a new bug into my FireBee. I had read before that FireTOS is the more general purpose TOS that offers some backwards compatibility and EMUTOS is the pure ColdFire TOS. This requires ColdFire Binaries for it to work and does not give you USB Support by default. It is dicussed here: http://firebee.org/fb-bin/page?label=fb_selecting_the_os&lng=EN though the translation in my opinion is not totally clear. Just too much information and a poor choice on my part. But a great learning experience for me and others.

As user wongck on the forum so obviously pointed out My advice is.... seems too late now anyway.... not to try to change too many things. Lately that s what I had done was too many changes but worse not clearly stating exactly what I want from the FireBee when asking for assistance on the Forum. It was obvious to me but not always to others

Anyway, Happy New Year and until next week.

Firebee News Update, 2 - New Boards Ordered

Medusa Computer Systems has started the order transaction for the new series of FireBee boards.

The computers will be built, as already the former products by MCS, at a swiss assembling company. At present we are waiting for a definitiely day of delivery.

The new FireBee computers can be ordered furthermore. Who likes to pay by two instalments can presently still make a deposit, until the completion of the new series. All those who preordered will be contacted by us in time, before the delivery and asking for (final) payment, for ordering possible additional requests like PSUs, CF cards, mini cases right away.

We wish the entire community happy holidays, and will keep you up to date in the new year.

Eureka Lite

By Francois Le Coat

Happy New Year,

For 30th ATARI ST anniversary, I thought it would be a good idea to build a lite version of Eureka 2.12, that can run in 1Mb of memory. So the 2D Graph Describer and 3D Modeller can start on early ST, STf, STe
etc.

<http://eureka.atari.org/eurklite.zip>

That version fits on a 720Kb floppy drive, and requires 1Mb of

RAM. Eureka 2.12 is a 2D graph visualization and 3D modelling software.

Enjoy, it’s yours =)

--
François LE COAT
Author of Eureka 2.12 (2D Graph Describer, 3D Modeller)
http://eureka.atari.org/

=~=~=~=

->In This Week’s Gaming Section - Hackers Shut Down EA and Steam Servers!
Rise of the Tomb Raider Coming to PC!
New Atari Jaguar Controller In Development!
And more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!

Hackers Shut Down EA and Steam Servers Because It s Christmas

Last week HR reported about a hacking group Phantom Squad that is planning ruin holidays for the gamers. It looks like the group has started working on turning their plans into reality However, another group known as SkidNP has also joined the attacks and shut down Steam servers.

The group Phantom Squad has targeted EA (Electronic Arts) server with very severe attacks and a number of users of reported problems in accessing the PSN servers.

EA also confirmed the attacks via twitter and apologized for any inconveniences.

You may have some difficulty launching games, applications, or online features. Our engineers are working to resolve the issue as soon as possible, and we thank you for your patience. One of the tweets said.

Right after the announcement from EA, the hacking group stopped the attacks and also announced the attacks on their twitter account. The attack lasted 3 hours and jolted the EA server badly.

The tweets from hackers can t be posted here as twitter has already suspended their account.

But, this is not the first attack from the group previously they attacked all the popular games these days i.e. The Old Republic, Grand Theft Auto 5, Call of Duty: Black Ops 3, and Call of Duty: Black Ops 2. Though, these attacks were small and seemed to have been carried out for testing purposes only, but results acquired from those attacks can be used for a bigger attack later on.

Just a few days back the Phantom Squad joined hands with VandaSec and PhantomSec making the group much stronger.

So, for gamers, a difficult time has already started, just like last year when LizardSquad launched DDoS attacks on Xbox and PSN and users were not able to enjoy gaming during the holiday.

It would be interesting to see how leading gaming service providers cope with these attacks in upcoming days as this is a just a start and these hacking groups might come hard as the holiday season progresses.

Steam Servers:

The group targeting Steam server goes by the handle of SkidNP. Earlier today, gamers using steam service tweeted that they are facing a worldwide outage.

Rise of the Tomb Raider Coming to PC in January

According to Steam, Rise of the Tomb Raider will be available on the PC sometime in January.

Although this isn’t an official release date, it does correspond with previous reports. Back in July, Square-Enix announced that the game would be released on PC in early 2016. Two weeks ago, a listing on Amazon France had the game set for release on January 29, 2016. The Baba Yaga DLC is also set to come out in January, which would coincide perfectly with a PC release date for that month.

Given all of this information, it’s safe to assume the game will indeed be released on PC in January, though we don’t have an exact day for its release yet.

Rise of the Tomb Raider was announced during Microsoft’s Gamescom briefing in 2014 as a "2015 holiday exclusive" for the Xbox 360 and Xbox One, though some were confused as to whether or not the game would be coming to other platforms. Shortly afterwards, Microsoft head Phil Spencer clarified that the game was in fact a timed exclusive, which meant that it would eventually be released on other platforms in the future.

In addition to revealing the PC launch window, Square-Enix also announced that the game would come to Sony’s PlayStation 4 console sometime during the 2016 holiday season.

Where To Sell Back Your Unwanted Video Games

Poor Aunt Myrtle. She tried. She really did. But despite her best efforts, there’s just no way you can work up excitement over Just Dance 2016 when you were hoping for Just Cause 3.

The goood news? Once she has toddled back to Cleveland and you don’t have to worry about hurting her feelings, you have plenty of options when it comes to getting rid of the game and getting what you really wanted for Christmas.

Of course, in the best of all worlds, your present came with a gift receipt, letting you return it with little to no hassle. But if not, there are still a number of different ways to get cash or credit for that unwanted title. Getting the most take a little work, though.

GameStop: Still worth it?

When it comes to game trade-ins, GameStop is the big fish in the slightly-larger-than-it-was-a-few-years-ago-but-still-pretty-small pond. You can get cash for your old games, but it’s a sucker’s bet. The smarter play assuming you intend to purchase another game at some point is taking store credit.

To get the most credit, though, you’ll need to complete two steps. First, spend the $15 to join the store s PowerUp Rewards program (you’ll also get a subscription to Game Informer magazine, so it’s not lost money). Then, scan the store circulars and online ads, along with the forums of deal-centric websites like CheapAssGamer.

PowerUp Rewards members get more for their trades, sometimes several dollars per title. And in the post-holiday period, GameStop typically offers extra in-store credits for hot titles. Get rid of some biggies and you can potentially earn nearly double the credit you normally would.

Curious about how much you’ll actually receive for your title? GameStop lists what it offers for hot titles and hardware.

Competition has driven up the trade value of several titles. Many big box retailers that sell games also accept trades-ins as well. The good news with these outlets is you can also easily see who’s paying what (for in store credit, as none offer cash) before you bring your games in. Just head to the websites of WalMart. Best Buy, and Target to get a pretty reliable estimate.

As an added bonus, you can also use the credit you get for games for any items sold at those stores, so if you’re in need of a spare controller or even a new TV those unwanted games can help offset the cost.

If you’re a little more patient on when you actually receive the credit, Amazon’s trade-in program is an option worth considering. The service is pretty straightforward: Enter the titles you want to dispose of on the site and you ll see their trade value. Assuming that s acceptable to you, you print out a free shipping label, box them up, and drop them off at the nearest UPS location.

A week or so later, your Amazon account will receive a credit in that amount which, as with the brick and mortar kings, you can use on anything the site carries.

Another delayed gratification option is eBay. And, frankly, if you're looking for cash, this is your best bet. You have the ability to set minimum pricing and can even dictate the terms of payment. The risks, of course, include failing to find a buyer or being forced to accept a bid for an amount lower than you were hoping for.

So who's paying what? Prices vary frequently, so you'll need to do your homework. Here, however, is a look at what a few retailers were paying out for a handful of hot titles one week before Christmas:

Call of Duty: Black Ops III (PS4)

GameStop: $20 cash/$25 credit ($22/$27.50 for PowerUp Rewards members)

WalMart: $25.59

Best Buy: $27

Target: $25

Amazon: $23.77

Fallout 4 (PS4)

GameStop: $20 cash/$25 credit ($22/$27.50 for PowerUp Rewards members)

WalMart: $30.55

Best Buy: $29

Target: $25

Amazon: $26.55

Super Smash Bros. (Wii U)

GameStop: $20 cash/$25 credit ($22/$27.50 for PowerUp Rewards members)

WalMart: $23.60

Best Buy: $27

Target: $25

Amazon: $23.87

Halo 5: Guardians (Xbox One)

GameStop: $17.60 cash/$22 credit ($19.36/$24.20 for PowerUp Rewards members)

WalMart: $29.15

Best Buy: $25

Target: $25

Amazon: $19.67

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

New Atari Jaguar Controller In Development

One of the main criticisms levelled at Atari's Jaguar system is that the controller is an absolute mess. Waiting in line behind the lack of decent software, unconvincing 64-bit graphics (even though it is a true 64-bit system on a technical level) and poorly marketed CD add-on, the controller takes a lot of unwarranted flack.

Gamers who have wielded the Jaguar's controller will attest that it is actually rather comfortable to hold and, contrary to visual perception, doesn't have much weight. Furthermore, the D-pad is solid. There are also a lot of fantastic games on the system, but I digress. Sure, the lack of shoulder buttons on the stock controller is inexcusable but the Jaguar Pro Controller remedies that omission.

It appears that Jaguar modder 10p6, creator of the the Jaguar/Jaguar CD combo the Jaguar PlayOne also has the same opinion, and has set about creating the ultimate replacement: a Jaguar/Atari 5200 compatible controller with a built-in 'spinner' that can be used with titles such as Tempest 2000. Also featuring a fully integrated keypad, dual analogue sticks, shoulder buttons and a D-Pad, this could be the ultimate controller for Jaguar enthusiasts and the peripheral to finally silence the naysayers. In his own words, 10p6 describes the new controller design:

"The idea of this project is to make a controller for the 5200 and Jaguar that is ergonomic, innovative, functional and very reliable using off the shelf parts when possible. The case for the unit will be initially 3D printed, but it has also been designed so it can easily be duplicated in resin. The keypad is designed to use a Jaguar Numeric Membrane, or possibly a custom one of the same size and similar speck.

"Innovative parts of this controller are the analog sticks and spinner. The sticks are off the shelf parts that are reliable and functional, and are included to replace the awful 5200 analog stick, but hopefully could be implemented for Jaguar games.

"The spinner / rotary controller is something that has been done on the Jaguar numerous times. I did this on a previous controller where I made a removable spinner that could be placed in the center of the D-Pad. Even though this was functional and cool, it was a little impractical; others have done spinners that are either huge, crammed in an awkward space, or sacrifice a controller just for rotary control.

"My spinner is innovative as it is located around the D-Pad in a way that does not effect D-Pad functionality, but allows the spinner to be easily turned with a thumb or fingers. The hard part is designing controls that allow the D-Pad to rock, and the spinner to spin, but not to impede each other. In the photos you will see I used an approach that makes the D-Pad effectively appear as a pivot in a large circle, of which the spinner is then sandwiched between the spinner and the case; this allows the spinner to have horizontal rotation, while allowing the D-Pad to have vertical pivot. The notches in the Spinner are designed to allow a twin photo-interrupter to work.

"This is the same system as used in old ball mouse s. Here it allows for very accurate rotation, is very reliable, but reduces friction compared to systems that use mechanical potentiometers. Not shown on the renders, but included in the finished controller will be a simple slider switch that locks the spinner in place when not being used.

"The case is also partially designed (not for a specific screen) to allow the numeric KeyPad to be removed and replaced with a touch screen, maybe hooked up to Arduino or Raspberry Pi system board. This could allow for custom button mapping, electronic 5200 and Jag overlays, video input, handheld games systems, wireless functionality and so on. Note that this is a big controller, it is as long as a Lynx 2 and a little wider. It is designed for comfort and function over design."

There is no solid release date for this new controller as yet, but the Pro Controller certainly has some competition on its hands.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Microsoft Pledges To Inform Users of State Surveillance, Account Hacking

Microsoft has pledged to inform users if their online communications are being targeted and monitored by government entities and state actors.

Following the trail blazed by Facebook, Twitter and Google, the

Redmond giant says the firm will notify users if any part of their Microsoft account - including Outlook.com email and OneDrive has been "targeted or compromised by an individual or group working on behalf of a nation state."

Microsoft already tells users when alerts flag up suggesting accounts have been hacked by third parties, but on Wednesday, Microsoft Vice President Scott Charney said the company is willing to take additional steps to protect the personal information of its users.

The company says the attention of "state sponsored" entities is dangerous as it is likely government or state-based hackers will have access to tools and resources beyond your homegrown hacker.

While quick to point out such attention doesn’t mean that Microsoft’s own security or systems are necessarily compromised when an alert is issued, it does mean that users should take extra precautions if they attract these sorts of characters.

Additional steps to ensure your accounts remain safe can include turning on two-step verification -- such as linking your account to your smartphone -- changing passwords regularly and keeping an eye out for suspicious activity through the "Recent Activity" page on your Microsoft account.

Another way to keep your personal data and accounts safe is a simple one -- be wary of opening suspicious emails and both clicking on links and downloading attachments held within. Known as phishing campaigns, fraudulent emails which deliver malware payloads on to victim machines or direct users to malicious websites are a common tactic used to steal user credentials as well as compromise their systems and overall privacy.

If Microsoft users receive an alert forewarning them of state interest in their account, this doesn’t automatically mean their accounts have been hacked. As explained by Charney:

> "If you receive one of these notifications it doesn’t necessarily mean that your account has been compromised, but it does mean we have evidence your account has been targeted, and it’s very important you take additional measures to keep your account secure.
>
> You should also make sure your computer and other devices don’t not have viruses or malware installed, and that all your software is up to date."

While Microsoft will not reveal the threat actors behind state-sponsored attacks or their methods - as the information may be "sensitive," -- the company will let you know when hacking attempts come from these sources.

The Redmond giant is not the only company to begin warning users of state-sponsored attacks in recent weeks. Earlier this month, Yahoo also joined the cause, pledging to tell account holders when their data is being targeted by state-based threat actors.

North Korea’s Red Star OS (Looks Like Mac OS X) Spies on Its Own People

North Korea has its own homegrown computer operating system that looks remarkably just like Apple s OS X, which not only prevents potential foreign hacking attempts but also provides extensive surveillance capabilities.

Two German researchers have just conducted an in-depth analysis of the secretive state’s operating system and found that the OS does more than what is known about it.

Dubbed Red Star OS, the operating system based on a Linux 2009 version called Fedora 11 limits its users to a government-approved view of the world and has the tendency to ’watermark’ files on USB sticks to track user s shuttling contraband material.

In short, whenever a user inserts a USB storage device containing photos, videos or other documents, into a computer running Red Star, the OS takes the current hard disk’s serial number, encrypts that number, and writes that encrypted serial into the file, marking it.

The purpose of watermarking files is to track who actually has the particular file, who created that file, and who opened it.

Researchers previously reported this watermarking feature after analysing Red Star OS, but Florian Grunow and Niklaus Schiess of German IT company ERNW GmbH currently presented dive into Red Star OS goes further.

Most of the Red Star’s unique features, including its own version of encrypting files, were designed to grant its makers complete control over the operating system, making it independent from any code that could be compromised and exploited by foreign intelligence services, the duo said as they presented their findings at the Chaos Communication Congress in Hamburg on Sunday.

The researchers analysed the latest third version of Red Star OS coming out around 2013 and it is clear that software is as authoritarian as the country that developed it.

"This is a full-blown operating system where they control most of the code," Grunow said as quoted by Reuters. Moreover, the OS rigorously resists any changes made by its user and closely monitors every move of a user.

The Red Star OS provides its own firewall, antivirus system and web browser point to internal North Korean servers, and even the encryption is custom-developed.

However, the small program included in the OS constantly monitors the computer for any changes made to the system files.

As a result, any attempt by a user to tamper with the operating system’s core functions, like disabling antivirus or firewall, would lead to the computer displaying an error message or rebooting itself.

Since, there is no sign in the OS of the kinds of cyber attack capability North Korea has been accused of, Red Star OS is also designed to crack down on the growing illegal exchange of foreign media content, including films, music or document files.

At the current, the duo has no information on how many computers in North Korea are using this operating system, as they found the OS from a website located outside the country, while visitors to North Korea say most computers there still use Windows XP.

Cyber Attack Brings Down BBC Website for Several Hours

A cyber attack officially known as a distributed denial of service attack took the BBC website and streaming service, iPlayer, offline on Thursday.

Visitors to the sites were greeted by an error message, Error 500 Internal Error, which stayed in place for around three hours.

The BBC initially described it as a technical issue. The press office tweeted: We re aware of a technical issue affecting the BBC website and are working to fix this now. We ll update you as soon as we can.

Explore the heart and soul of what drives some of the top creative minds in fashion, beauty, and style on their roads to success.

A distributed denial of service occurs when a site is bombarded with more traffic than it can sustain.

The issue allowed the Twitterati to have fun at the BBC s expense. #BBCDown was trending Thursday morning in the U.K., alongside #HappyNewYear. Some alluded to the fact that British navy submarines carrying nuclear weapons have been instructed that the BBC ceasing operation may be taken as a sign that Armageddon has occurred.

Anonymous Hacks Asia Pacific Telecommunity Against Internet Censorship in Asia

Anonymous hacker collective has attacked the official website of Asia Pacific telecommunity and defaced it in protest against growing plans for internet censorship in Asia.

The hackers gained access of the website s admin panel (running Drupal) and from there, leaked all the data stored on the website along with defacing the site with one of their own pages.

In an exclusive conversation with one of the Anonymous hackers behind the attack, HackRead was told that:

> Though, we the Anonymous hackers have conducted this attack

but we would like to mention that we were also joined by hackers from other groups, you can call it an operation conducted by World Hacker Team against censorship in Asia.

During recent years, many Asian countries have increased censorship following the Chinese government s lead. Thailand has been one of the active countries, but other countries are not far away. In the last couple of months, Anonymous hacked CAT Telecom Pcl, the premier telecommunication website of Thailand and National Police server against Internet censorship.

Recently, China s president (Xi Jinping), in a World Internet conference, emphasized on censorship being the right of every country.

In the same conference, the organization responsible for managing domain names, ICANN (Internet Corporation for Assigned Names and Numbers) promised full support in working on the new internet plan in which Chinese officials will have stronger say on how the organization works.

ICANN will be taking over IANA (Internet Assigned Numbers Authority) which is currently run by the US government and with that move Chinese government will be able to monitor the internet all around the world. This move will certainly make internet users nervous.

Anonymous, in order to draw the attention of the people, defaced the Asian community website and left the message on the website and YouTube for people to ponder on. With that, they also leaked data like emails, usernames, and hashed passwords on the website.

Though, this will not stop ICANN or the Chinese government from progressing with their plans but it will certainly create awareness among the general public regarding the world of internet s new order.

At the time of publishing this article, the targeted website was still hacked.

Somebody Offered Money to Raspberry Pi Foundation for Pre-Installing Malware

The Raspberry Pi is now gaining attention from malware distributors who want the popular mini-computers to deliver with pre-install malware.

The Raspberry Pi Foundation has made a shocking revelation that the charitable foundation has been offered money to install malware onto the Raspberry Pi machines before they were shipped out to users.

The Raspberry Pi is an extremely simple computer that looks and feels very basic, but could be built into many geeky projects. Due to the low-cost appeal of the Raspberry Pi, the Foundation has sold over 4 million units.

Just Last month, Raspberry Pi unveiled its latest wonder: The Raspberry Pi Zero a programmable computer that costs just $5 (or £4), may rank as the world's cheapest computer.

Last Wednesday, the Foundation tweeted a screenshot of an email in which "business officer" Linda effectively asked Foundation's director of communications Liz Uptonto to install a suspicious executable file onto Raspberry Pis for which the officer promised to offer a "price per install."

The email further explained that installing the executable file would create a shortcut icon on the user's desktop and opening the shortcut would take the user to the company's website. "Then this is our target," the email reads.

However, the name of the company represented by Linda was not revealed by the Raspberry Pi Foundation.

Obviously, the paid-for-malware distributor pitched the wrong organisation, who declined the offer, describing the company as "evildoers," but the incident once again raises the question about this common, widespread issue.

Decade Old Software Bug Sets 3000 US Prisoners Free

A software bug in Washington State Department of Corrections (DoC) has been handing freedom to the inmates well before their sentence was due to end Each year, over 3200 prisoners benefitted from this bug since 2002.

All this started when a Supreme Court amended the 1995 law on how to calculate release date mitigating prisoner s good behavior against time to be served which then necessitated an update to the software back in 2002. Once the software was updated against the Supreme Court s ruling the software began to calculate incorrect release dates.

Before the court s ruling, only time spent by an inmate in a state prison was considered and not the county jail time for calculating good time .

The error basically occurred due to enhancements which is an additional sentence period as a result of the violent nature of the crime like sexual assault, firearm crimes, weapon usage, etc.

Enhancements, by law, are not to be counted up against a good time. However, the software did just that. It added the enhancement as total prison time with the county jail time which made the software show higher values for any inmate who was to be given early release against the good time .

This bug was originally identified back in 2012 when an assault victim s family identified the incorrect release of the inmate. Once they reported this to DoC, the officials asked for a system-wide update as a priority but for unknown reasons it was delayed until November 2015 when DoC hired an IT expert who identified how big the bug was.

55 days on average

According to the findings from the IT experts, on average a prisoner was released 55 days before his actual date and about 3200 prisoners each year benefitted.

DoC is now tracking down the inmates who benefited to make them complete their time in prison and is also working on fixing the bug.

Governor Inslee has hired Robert Westinghouse and Carl Blackstone and two retired federal prosecutors for reviewing this incident. Inslee in a statement said:

That this problem was allowed to continue for 13 years is deeply disappointing to me, totally unacceptable and, frankly, maddening, Inslee said.

Microsoft Keeps Backup of Your Encryption Key on Its Server Here's How To Delete It

Have you recently purchased a Windows computer?

Congratulations! As your new Windows computer has inbuilt disk encryption feature that is turned on by default in order to protect your data in case your device is lost or stolen.

Moreover, In case you lost your encryption keys then don't worry, Microsoft has a copy of your Recovery Key.

But Wait! If Microsoft already has your Disk Encryption Keys then what s the use of using disk encryption feature? Doesn't Encryption mean Only you can unlock your disk?

Since the launch of Windows 8.1, Microsoft is offering disk encryption as a built-in feature for Windows laptops, Windows phones and other devices.

However, there is a little-known fact, highlighted by The Intercept, that if you have logged into Windows 10 using your Microsoft account, your system had automatically uploaded a copy of your recovery key to Microsoft s servers secretly, and you can't prevent device encryption from sending your recovery key.

Note: Do not get confuse device encryption with BitLocker. Both works same but have different configuration options. BitLocker offers users a choice whether or not they want to backup their Recovery keys on Windows server.

Why Should You Worry?

- If a hacker hacks your Microsoft account, he can make a copy of your recovery key before you delete it (method described below).
- Any Rogue employee at Microsoft with access to user data can access your recovery key.
- If Microsoft itself get hacked, the hacker can have their hands on your recovery key.

Even Law Enforcement or Spy agencies could also request Microsoft to hand over your recovery key.

"Your computer is now only as secure as that database of keys held by Microsoft, which means it may be vulnerable to hackers, foreign governments, and people who can extort Microsoft employees," said Matthew Green, a cryptography professor at Johns Hopkins University.

How to Delete your Recovery Key from your Microsoft Account?

Although there’s no way to prevent a new Windows computer from uploading the recovery key at the very first time you log into your Microsoft account, you can delete the existing recovery key from your Microsoft account and generate a new one.

Follow these simple steps in order to remove your recovery key from your Microsoft account:

Step 1: Open this website and log in with your Microsoft Account

Step 2: You will find list of recovery keys backed up to your Microsoft Account

Step 3: Take a back of your recovery Keys locally

Step 4: Go ahead and delete your recovery key from Microsoft Account.

Important Fact: Green also pointed out that even after deleting the recovery key from your Microsoft account, there is no guarantee that the key has been removed from the company’s server.

Instant Solution: To solve this issue, Windows users are recommended to stop using their old encryption keys and generate a new one without sharing it with Microsoft.

How to Generate a New Encryption key (Without Sending a copy to Microsoft)?

Sorry for Windows Home Edition users, but Windows Pro or Enterprise users can create new key by decrypting whole hard disk and then re-encrypt the disk, and this time in such a way that you will actually get asked how you want to backup your Recovery Key.

Step 1: Go to Start, type "Bitlocker," and click "Manage BitLocker."

Step 2: Click "Turn off BitLocker" and it will decrypt your disk.

Step 3: Once done, Click "Turn on BitLocker" again.
how-to-install-bitlocker

Step 4: Then Windows will ask you: How you want to backup your Recovery Key. Make sure to DO NOT SELECT "Save to your Microsoft Account." That’s it.

Congratulations!

Finally, the new Windows device you purchased specially for disk encryption feature has now enabled the feature, and Microsoft no longer can unlock it.

Microsoft Failed To Warn Victims of Chinese Email Hack

Microsoft Corp experts concluded several years ago that Chinese authorities had hacked into more than a thousand Hotmail email accounts, targeting international leaders of China s Tibetan and Uighur minorities in particular but it decided not to tell the victims, allowing the hackers to continue their campaign, according to former employees of the company.

On Wednesday, after a series of requests for comment from Reuters, Microsoft said it will change its policy and in the future tell its email customers when it suspects there has been a government hacking attempt. Microsoft spokesman Frank Shaw said the company was never certain of the origin of the Hotmail attacks.

The company also confirmed for the first time that it had not called, emailed or otherwise told the Hotmail users that their electronic correspondence had been collected. The company declined to say what role the exposure of the Hotmail campaign played in its decision to make the policy shift.

The first public signal of the attacks came in May 2011, though no direct link was immediately made with the Chinese authorities. That’s when security firm Trend Micro Inc announced it had found an email sent to someone in Taiwan that contained a miniature computer program.

The program took advantage of a previously undetected flaw in Microsoft s own web pages to direct Hotmail and other free Microsoft email services to secretly forward copies of all of a recipient s incoming mail to an account controlled by the attacker.

Trend Micro found more than a thousand victims, and Microsoft patched the vulnerability before the security company announced its findings publicly.

Microsoft also launched its own investigation that year, finding that some interception had begun in July 2009 and had compromised the emails of top Uighur and Tibetan leaders in multiple countries, as well as Japanese and African diplomats, human rights lawyers and others in sensitive positions inside China, two former Microsoft employees said. They spoke separately and on the condition that they not be identified. Some of the attacks had come from a Chinese network known as AS4808, which has been associated with major spying campaigns, including a 2011 attack on EMC Corp’s security division RSA that U.S. intelligence officals publicly attributed to China. To see the report click here: http://www.secureworks.com/cyber-threat-intelligence/threats/sindigoo/

Microsoft officials did not dispute that most of the attacks came

from China, but said some came from elsewhere. They did not give further detail.

"We weighed several factors in responding to this incident, including the fact that neither Microsoft nor the U.S. government were able to identify the source of the attacks, which did not come from any single country," the company said. "We also considered the potential impact on any subsequent investigation and ongoing measures we were taking to prevent potential future attacks."

In announcing the new policy, Microsoft said: "As the threat landscape has evolved our approach has too, and we ll now go beyond notification and guidance to specify if we reasonably believe the attacker is ‘state-sponsored.’" Requests for comment from China s Foreign Ministry and the Cyberspace Administration of China were not immediately answered. The Chinese government routinely issues strong denials of involvement in all hacking activities.

After a vigorous internal debate in 2011 that reached Microsoft s top security official, Scott Charney, and its then-general counsel and now president, Brad Smith, the company decided not to alert the users clearly that anything was amiss, the former employees said. Instead, it simply forced users to pick new passwords without disclosing the reason.

The employees said it was likely the hackers by then had footholds in some of the victims’ machines and therefore saw those new passwords being entered.

One of the reasons Microsoft executives gave internally in 2011 for not issuing explicit warnings was their fear of angering the Chinese government, two people familiar with the discussions said.

Microsoft s statement did not address the specific positions advocated by Smith and Charney. A person familiar with the executives thinking said that fear of Chinese reprisals did play a role given the company’s concerns about the potential impact on customers.

Microsoft said the company had believed the password resets would be the fastest way to restore security to the accounts.

"Our primary concern was ensuring that our customers quickly took practical steps to secure their accounts, including by forcing a password reset," the statement said.

It is unclear what happened to the email users and their correspondents as a result of Microsoft’s failure to alert them to the suspected government hacking. But some of those affected said they were now deeply worried about the risks, especially for those inside China.

 The Internet service providers and the email providers have an ethical and a moral responsibility to let the users know that they are being hacked, said Seyit Tumturk, vice president of the World Uyghur Congress, whose account was among those compromised. We are talking in people s lives here.

Unrest in Xinjiang, the Chinese region bordering Kazakhstan that is home to many Uighurs, has cost hundreds of lives in recent years. Beijing blames Islamist militants, while human rights groups say harsh controls on the religion and culture of the Uighurs have led to the violence.

Until Wednesday, Microsoft had rejected the idea of explicit warnings about state-sponsored hacking, such as those Google Inc. began in 2012, the former employees said. In the 2011 case, the company also opted not to send a more generic warning about hacking. Yahoo Inc and Facebook Inc have been issuing such warnings for several years, former employees of those companies told Reuters, including when the principal suspect was a government. Both companies, along with Twitter Inc, announced in recent months that they would follow Google s lead and explicitly notify users about suspected state-sponsored hacking.

Google said on average it now issues tens of thousands of warnings about targeting every few months, and that recipients often move to improve their security with two-factor authentication and other steps.

Reuters interviewed five of the Hotmail hacking victims that were identified as part of Microsoft s investigation: two Uighur leaders, a senior Tibetan figure and two people in the media dealing with matters of interest to Chinese officials.

Most recalled the password resets, but none took the procedure as an indication that anyone had read his or her email, let alone that it may have been accessed by the Chinese government. I thought it was normal, everybody gets it, said one of the men, a Uighur ØmigrØ now living in Europe who asked not to be named because he left family behind in China.

Another victim identified by Microsoft s internal team was Tseten Norbu of Nepal, a former president of the Tibetan Youth Congress, one of the more outspoken members of a community that has frequently clashed with Chinese officials. Another Microsoft-identified victim was Tumturk, the World Uyghur Congress vice president who lives in Turkey. Microsoft investigators also saw that emails had been forwarded from the account of Peter Hickman, a former American diplomatic officer who arranged high-profile speeches by international figures at the National Press Club in Washington for many years.

Hickman said he used his Hotmail account on Press Club computers to correspond with people, including the staff for the Tibetan government in exile, whose leader Lobsang Sangay spoke at the club in 2011; Tumturk’s World Uyghur Congress, whose then-president Rebiya Kadeer spoke in 2009; and the president of Taiwan, who spoke by video link-up in 2007. Hickman said he didn t recall the password reset. He said he never suspected anything was wrong with the account, which he continues to use.

AVG Antivirus Broke Chrome s Security, and Google s Furious About It

AVG Antivirus has been a popular security suite for more than a decade. The company claims more than 200 million active devices, including 100 million mobile installations. Over the past few years, the company has come under increasing fire for installing its AVG SafeSearch toolbar without permission, and announcing that it would sell consumer data to advertisers. Now, the company may have finally gone too far, thanks to an enormous bug in its AVG Web TuneUp software that fundamentally broke security for Google Chrome users.

On December 15, Google Security researcher Tavis Orlandy filed a bug report with AVG, noting that the software:

[A]dds numerous JavaScript API s to chrome, apparently so that they can hijack search settings and the New Tab page. The installation process is quite complicated so that they can bypass the Chrome malware checks, which specifically tries to stop abuse of the extension API.

Orlandy followed up the bug report with a self-described angry email sent directly to AVG. In it, Orlandy writes:

I m really not thrilled about this trash being installed for Chrome users. The extension is so badly broken that I m not sure whether I should be reporting it to you as a vulnerability, or asking the extension abuse team to investigate if it s a PuP [potentially unwanted program].

Nevertheless, my concern is that your security software is disabling web security for 9 million Chrome users, apparently so that you can hijack search settings and the new tab page.

There are multiple obvious attacks possible, for example, here is a trivial universal xss in the navigate API that can allow any website to execute script in the context of any other domain. (The relevant code samples can be viewed at the initial bug report.)

AVG released a broken patch for the problem on December 19, which Google promptly rejected. The company revised its patch again, but as of December 28, Google is reviewing the extension to determine if AVG will be allowed to offer it at all.

A review of the most recent anti-virus comparisons at AV-Comparatives shows AVG s anti-virus performing at the top of the heap. The same cannot be said, however, for the foistware that the company has taken to pushing at its users. A litany of user complaints have erupted in recent years, most of which say the same things: AVG s supplementary software Web TuneUp, SafeSearch, and the like are security disasters and rampantly disliked.

The fact that the company now wants to sell consumer data (the information above is from AVG itself) may just be the last straw for many users. AVG has traded actual due diligence for pushing users towards products that don t function while selling the data of its userbase.

Stop Sharing This Bogus Facebook Post. It Won’t Make You Rich

There are always rumors and hoaxes spreading on Facebook.

The latest myth comes in the form of a chain letter. It claims that CEO Mark Zuckerberg will distribute $4.5 billion worth of his Facebook shares among 1,000 people who copy and post the letter. Of course, this is completely bogus - and Facebook has stated as much -- but that hasn’t stopped the hoax from spreading.

As reported by Tech Insider, it began circulating in early December, right after Zuckerberg and his wife Priscilla announced that they would give away 99 percent of their Facebook shares to the Chan Zuckerberg Initiative, a philanthropic LLC that will funnel its earnings into nonprofits "to advance human potential and promote equality."

Hours after their announcement, the hoax started gaining popularity.

Here’s a version of the status that people are sharing:

> Mark Zuckerberg has announced that he is giving away $45 billion of Facebook stock. What you may not have heard is that he plans to give 10% of it away to people like YOU and ME! All you have to do is copy and paste this message into a post IMMEDIATELY. At midnight PST, Facebook will search through the day’s posts and award 1000 people with $4.5 million EACH as a way of saying thank you for making Facebook such a powerful vehicle for connection and philanthropy.

Facebook immediately debunked this in an official statement, reminding users that "not everything you read on the Internet is real."

Nonetheless, the message resurfaced this week.

Certainly, Facebook and other social networks provide fertile ground for hoaxes and scams to quickly gain momentum. Every so often, rumors circulate claiming that Facebook is going to start charging users or that people can now tell when you’ve looked at their profile. Of course, these rumors are all false.

The lesson here is simple. Don’t believe everything your friends share on social media. And, when in doubt, check Facebook’s official page or the site’s Terms of Service - they’ll protect you from being duped.

Kim Dotcom Loses Fight Against Extradition to the US

Internet millionaire and Megaupload founder Kim Dotcom and his three associates are eligible for extradition to the US to face criminal charges over massive copyright infringement on Megaupload (now-shuttered), the court has ruled citing

"overwhelming" evidence.

On Tuesday afternoon, New Zealand District Court Judge Nevin Dawson told the court that the United States had presented enough evidence against Dotcom and his co-defendants and that they should be surrendered to the US.

US prosecutors want Dotcom, and colleagues Mathias Ortmann, Bram van der Kolk and Finn Batato to stand trial on charges of copyright infringement, racketeering, and money laundering.

"No matter what happens in Court tomorrow, I'll be fine. Don't worry. Enjoy your Christmas & know that I'm grateful to have you, my friends," Dotcom tweeted before the court hearing.

The court ruling comes almost three years after the New Zealand police raided Dotcom's Auckland mansion at the request of the FBI and in the same year the US government launched extradition proceedings.

It was a high-profile armed raid, but it has taken almost four years for the courts to reach a decision on whether to send Dotcom to America.

Officials say Dotcom's file-sharing service Megaupload served copyright contents, including music, movies, electronic books, television programs, as well as business and entertainment software on 'a massive scale.'

The US government estimates the harm to film studios and record companies was more than $500 Million (£322 Million).

However, Dotcom and three defendants now have 15 days to appeal the court ruling.

"Justice was not served today," Dotcom's California-based lawyer Ira Rothken tweeted, confirming their plans to appeal the US extradition request in the High Court.

"The @KimDotcom team looks forward to having the US request for extradition reviewed in the High Court. We have no other comments at this time," Rothken said.

However, the defendants are allowed to remain out on bail in the meantime. Although the judge insisted that all the defendants should be ordered to report to probation every day.

BlackBerry's Pakistan Operations To Continue After Government Drops Access Demands

BlackBerry won't be pulling out of Pakistan after all. The local government has rescinded its shutdown order and dropped its request for access to BlackBerry Enterprise Server (BES) email and messaging content. A new post from Marty Beard, BlackBerry's Chief Operating Officer, revealed that the two reached an agreement, and that the Pakistani government was able to accept BlackBerry's position on security.

We are grateful to the Pakistan Telecommunication Authority and the Pakistani government for accepting BlackBerry's position that we cannot provide the content of our customers' BES traffic, nor will we provide any so-called backdoors to our BES servers.

BlackBerry looks forward to serving the Pakistani market for years to come, including introducing new products and services, and thanks our valued customers in Pakistan for their patience and loyalty.

Security is something that BlackBerry values, and it is good to see the company stand firm on its beliefs. BlackBerry says it is willing to assist law enforcement agencies in investigations of criminal activities, but the company is not about handing out back door access to its private information.

R.I.P Ian Murdock, Founder of Debian Linux, Dead at 42

Ian Murdock, the founder the Debian Linux operating system and the creator of apt-get, has passed away.

Yes, it is very sad to announce that Ian Murdock is not between us. His death has touched the entire software community. He was just 42.

The announcement of Murdock death came out via a blog post on Docker website, where Murdock was working as a member of the technical staff.

The cause of death is unclear at present, but Murdock tweeted the same day that he would commit suicide that night. His Twitter account had since been deleted.

However, at that time, some people speculated that Murdock s account had been hacked and that the tweets were not by him.

Murdock posted some Tweets on Monday suggesting he had been involved in a police case and has been beaten by the police and charged with battery.

However, neither Docker, nor the San Francisco Police Department immediately commented on Murdock s actual cause of death.

Murdock developed Debian in August 1993 and yes the ian in the project s name is from Ian Murdock.

In the past, He also worked at Sun Microsystems and served as the CTO of the Linux Foundation.

It is with deep regret that we say goodbye to our great friend, the most significant contributor to Linux community, our beloved Ian Murdock.

Rip :(

U.S. Broadband Speeds Tripled in 3.5 Years

In an effort to keep up with an increasingly data-dependent society, U.S. broadband speeds have tripled over the past 3.5 years.

The Federal Communications Commission's fifth Measuring Broadband America report, released Wednesday, said average download speeds increased to nearly 31 megabits per second (Mbps) in September 2014 up from 10 Mbps in March 2011.

In recent years, companies like Google, AT&T, and Comcast have begun offering speeds of up to 1,000 Mbps (or more), elevating them high above the FCC's redefined broadband benchmark of 25 Mbps.

Rising Internet speeds satisfies customers streaming videos, playing games, and downloading data every day. Citing recent Cisco data, the Commission said video traffic currently accounts for more than 60 percent of Web traffic. That's expected to grow to 80 percent by 2019.

"[This] report confirms that advances in network technology are yielding significant improvements in broadband speeds and quality," FCC Chairman Tom Wheeler said in a statement. "Faster, better broadband will unleash new innovations and new services to improve the lives of the American people."

But the U.S. is still lagging behind the rest of the world. We ranked 25 out of 39 nations in 2013, falling behind countries like France, Canada, Germany, and Japan, Reuters said.

In the fall, New York Attorney General Eric Schneiderman launched an investigation into whether Verizon, Cablevision, and Time Warner Cable deliver advertised speeds.

And, the FCC in June fined AT&T $100 million for failing to adequately explain to customers of its "unlimited" data plans how much their service would be throttled after a certain amount of data use.

Meanwhile, Akamai's State of the Internet report released earlier this month suggested that global Internet connection speeds were up 14 percent in the third quarter to a measly 5.1 Mbps.

How Google Is Learning From Past Mistakes With New Version of Glass

Nearly one year after Google pulled sales of its consumer version of Google Glass, its team is back with plans for a revamped version of the futuristic eye wear that fixes previous concerns about privacy and portability.

While no release date has been set, the latest filings from Google posted this week on the Federal Communications Commission's website

show how the company addressed the biggest concern that dogged the first edition of Glass -- its camera.

The new plans for Glass include a green light that will turn on when a user is recording video, according to the FCC filings.

Restaurants, movie theaters and strip clubs had banned the device over concerns users could surreptitiously use the eye wear to record video.

"With the first version of Glass, users were shunned and mocked to the point that owners stopped wearing them," Patrick Moorhead, an analyst at Moor Insights and Strategy, told ABC News. "Google learned the hard way that users don’t want anonymous videos or photos taken of them and therefore on the new version, they added a light when the camera is in use."

The filings also show Google has tweaked the design of Glass by moving the power button to the back of the glasses. Another key change includes a hinge, making it easier to fold Glass and presumably slip it into a smaller carrying case that could perhaps fit into a small bag or even someone’s front pocket. The first edition of Glass required users to carry around a larger hard case.

The latest plans for Glass are reportedly aimed at business users instead of everyday consumers. While Google has made some design tweaks, Moorhead said "size and style aren’t as big of an issue" with the latest version.

Glass went on sale to the public in May 2014 for $1,500. Earlier this year Google vowed that the public would see a next generation of Glass. Less than a year later, it appears Google is making good on that promise.

Glass is a part of Google X. Google X is a subsidiary of Google’s parent company Alphabet.

What Will The Internet Of Things Be When It Grows Up?

An old proverb advises, Keep a thing seven years, and you ll find a use for it. Well, it s been about seven years since there were officially more things connected to the Internet than people. It looks like they re keepers, and we ve found countless uses for them.

Now that the Internet of Things (IoT) seems to be firmly embedded in our lives, 2016 may be that transformational year when it segues from the gee whiz arena into practical, everyday application along with all that entails in regard to development, policy and standards.

Here are some predictions for the IoT as it matures in 2016

The same material science that is improving the range of the electric car will increase the duration of battery life for connected devices. This is a pretty important development, and

will herald a larger number of wireless IP-based devices. And with this increase in numbers, more thing makers will start to offer direct-access APIs to their devices on local networks for other trusted IP-based devices (as opposed to offering exclusive access only through the cloud).

I am also anticipating the emergence of more natural interactions between people and things in the coming year making devices more usable via voice control and semantic modeling and social interplay. This will create thing interactions that present less friction between people and technology, which is a prerequisite on the march toward IoT ubiquity.

On the visual human/thing-interaction front, we can also expect hologram technology to accelerate in 2016. A selection of APIs, SDKs and new gear will emerge next year and really kick off widespread development of hologram-based cards and similar applications.

> The IoT is not a revolution in technology, but rather an evolution.

One sticky development that may arise next year concerns the IoT and microdrones, as I think smaller form-factor personal drones will start to appear in 2016 (and like smartphones, they ll be equipped with high-quality cameras and streaming capabilities). With these new IoT devices, people will begin to record, contextualize, share and store the droneable moments of their lives.

Other people s privacy will be of significant concern, but will not stop the spread. Video will be captured and analyzed to create actionable data that s cross-referenced with simultaneous or near-simultaneous contextual events (by time, location, subject participation, perspective, device density, etc.).

Determining who controls all that data and what is done with it will lead us down some interesting paths; debates about our current selfie-mania and mass over-sharing on social media will pale by comparison. Which leads us to
Policy

Privacy issues will come to the fore as big players around the world increase their supply of IoT data-collecting devices and services. Legal jurisdictions will start to impose more rules that are more favorable to the preservation of consumer privacy by restricting where and how data can be extracted, moved, analyzed and traded. I also wouldn t be surprised to see a few class actions or criminal litigation actions stemming from these issues.

Sadly, I think privacy and security failures by several large IoT providers in the new year will be a catalyst for this increased awareness. IoT devices, networks and infrastructure are already targets for nefarious threat actors, but I think the coming year will be marked by at least a few dramatic IoT hacks.

As the IoT evolves in industries such as transportation and healthcare, for example, policies around privacy and security will become a much more pressing concern. 2016 may be the year in which widespread foundational legal and administrative

protocols are laid for the IoT. As part of that process
Standards

In 2016, a certifying authority will begin to form so that some level of trust can be converted and conveyed to boost consumer confidence as they hire new IoT devices in their lives. This authority will most likely employ an easy-to-understand confidence badge certifying that devices comply with a minimum level of security and data protection.

I also think that a dominant schema will become evident next year, which will serve as the suggested dictionary, and that much of the industry will choose to follow it. This schema will be treated as open source, so individuals and companies around the world can participate in its evolution.

And at least two more new communications standards will emerge next year (maybe even one from a large retailer building its own broad IoT platform). Both will seek to gain worldwide acceptance as THE standard for connectivity between things, people and processes, but it s hard to guess at this point whether either of them will actually fit the bill. So
Are We There Yet?

The IoT is not a revolution in technology, but rather an evolution. As such, things will continue to evolve in accordance with human notions about their uses and application. Currently, there is too much noise for the mass market to really understand IoT and the value it can bring to their daily lives.

That confusion is augmented by the variety of non-interoperable products laid out side-by-side on store shelves, and the lack of a dominant standard. There is still a long way to go before we can consider the IoT mature. But 2016 may be the year we get our first real glimpse of what a full-grown IoT will look like, and it s coming along nicely.

The Internet of Things Is Everywhere, But It Doesn t Rule Yet

In the future, everything will be connected. It won t just be our phones that access the Internet; it will be our light bulbs, our front doors, our microwaves, our comforters, our blenders. You can call it the Internet of Things, The Internet of Everything, Universal Object Interaction, or your pick of buzzwords that begin with Smart. They all hold as inevitable that everything, everything will be connected, to each other and to the Internet. And that will change the world.

Juniper research predicted that by 2020, there will be 38.5 billion connected devices. IDC says it ll be 20.9 billion. Gartner s guess? Twenty-five billion. The numbers don t matter, except that they re huge. They all agree that most of those gadgets will be industrial the Internet of Things is less about you changing the color of your lightbulb and more about companies large and small finding new ways of making their businesses, and your life, easier and more efficient. But the market for connecting the devices you use all day, every day, is about to be

huge.

2015 was the year everyone talked about the Internet of Things. (So was 2014. And 2013.) But unlike before, it was the year everyone started making plans, laying groundwork, and building the infrastructure for the day when all our devices are connected. It wasn t the year those devices took over our homes, but don t look now there are suddenly Trojan horses everywhere.

Did you buy an Apple TV this fall? You now have a Homekit hub in your house, and if you buy a HomeKit-enabled device it ll be incredibly easy to set up. Have an Amazon Echo? Try saying, "Alexa, turn the lights off." Actually, that one will only work if you have a Philips Hue set and you ve already done the work of setting things up. It s a whole thing.

Which brings us to the real dilemma the Internet of Things is facing as we come to the end of 2015: how the hell are all these things going to work together? Apple has Homekit; Google has Brillo and Nest; Microsoft has Windows; Samsung has SmartThings. There s Wemo and Wink and Zigbee and Z-Wave and Thread and I m not even making any of these up. You can control some things with your fitness tracker, some with a universal remote, and pretty much all of them with your phone. Some of the protocols overlap and support each other; others are more exclusive. But there s no simple plug-and-play option, no way to walk out of Best Buy with something you know is going to work.

Right now, says Frank Gillett, a vice president and analyst at research firm Forrester, people mostly buy single products for a single purpose. "It works if you have a specific headache," he says. "I want to lock my door, or I want to feed my pet." He calls these app-cessories. "As a shelf item in an Apple Store or Best Buy, it works. But if you want to make those things sing and dance together, forget it." Even these simple things aren t taking off yet: his research shows only 7 percent of Americans partake in even a single smart-home scenario.

Our homes are going to get smarter. But it s going to happen slowly, Gillett says, at the rate we d upgrade our homes anyway. "None of us want to go out and do home renovations just to get a dang smart home," he says. We won t run out just to buy a smart crock-pot or refrigerator, but the next time we re shopping for one which could be a decade from now we might buy the connected one.

Our smart homes and connected worlds are going to happen one device, one bulb at a time, not in a single motion. But companies know they have to get you into their platform with that first device, or risk losing you forever to someone else s closed ecosystem. If you bought a Nest thermostat and plugged it into your wall, odds are you re not switching to HomeKit anytime soon. (Or buying an Ecobee thermostat for upstairs.) The super-cool August Smart Lock works with HomeKit, but nothing else. It s not that they re completely mutually exclusive you can just use your phone to control everything but few things currently work together in that magical, my-home-just-gets-me way the Internet of Things has promised. Plus, your phone s a lousy remote for the physical world. "The idea that we re going to use our phone to

adjust the light is bonkers, Gillett says, because it s a lot harder to do it that way than hit the switch.

It s possible some regulatory body will decide on a set of standards, or everybody will agree to support everybody else and redundancy will rule the day and redundancy will rule the day. Or, maybe more likely, there will be a breakout smart-home product that finally gives a single platform enough clout to force others to play nice. That hasn t happened yet, and no one really knows what it ll be: a smart refrigerator that knows when you need groceries? A really great security system? There are so many nice products in the Internet of Things, but nothing mainstream enough to force the industry forward.

The technology is there. Connected light bulbs, connected tea kettles, connected fridges and fans and coffeemakers and cars it s all possible. It s not perfect, but the parts are only going to continue to get better, smaller, and cheaper. So the question is no longer, is it possible to connect everything to the Internet? Yeah, it s possible. The question now: How do we do it the right way? IoT companies need to set standards, pick both winners and losers, and come up with ways to make it easier for everyone to get on board.

In 2016, we ll need to begin grappling with the security concerns these devices raise having your Target account hacked is one thing, your car or home-security camera is another entirely. We ll have to understand the sheer volume and intimacy of the data we re handing over as we go about our hyper-connected lives, and hold our leaders and executives accountable for what they do with that data.

Know this, though: it may be coming like a molasses tidal wave, but the Internet of Things is coming. It s not a matter of if or whether, but when and how. 2015 was about starting to sort out what these devices will look like, how they ll work, how they ll work together, and how we ll make sure they don t ruin everything. The tracks have been laid. Maybe it ll be 2016, maybe the year after, but the train is coming. It ll have Wi-Fi and Bluetooth and probably eight other things, and you ll definitely get a push notification when it gets here.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without

the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.